IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 09/556,068 §
Filed: April 21, 2000 § Examiner: Patel, Haresh N.
Inventors: § Group/Art Unit: 2154
Sai V. Allavarpu, Xuesi Dong, Linda C. Lee § Atty. Dkt. No: 5181-48400
Title: Secure Access to Managed Network §
Objects using a Configurable §
Platform-Independent Gateway §

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Claims 1-63 are pending in the application. Reconsideration of the present case is earnestly requested in light of the following remarks. Applicants note the following clear errors in the Examiner's rejection. To save space, only the independent claims will be discussed herein.

The Examiner rejected claims 1, 20, 39 and 58-60 (and numerous dependent claims) under 35 U.S.C. § 102(e) as being anticipated by Vuong et al. (U.S. Patent 6,430,578) (hereinafter "Vuong") and also as anticipated by Spencer (U.S. Patent 6,253,243). Applicants respectfully traverse these rejections for at least the reasons presented below.

Regarding claims 1 and 58, Vuong and Spencer both fail to disclose a gateway which is coupled to a plurality of managed objects and which is configured to deliver one or more events generated by the managed objects to one or more managers or to deliver requests generated by the managers to one or more of the managed objects, as recited in claim 1. Vuong's name service is not coupled to a plurality of managed objects, nor does requesting that a name and/or address be inserted as an entry into the database, as the Examiner relies on, constitute *managing* the delivering of events or requests to managed objects. Spencer, cited at col. 5, lines 46-65, describes how management application 300 communicates with MIS server 306 via a portable management interface (PMI) 302, an object-oriented interface that provides access to management information without disclosing anything about a gateway providing object-level access control between managers and managed objects.

Vuong and Spencer also fail to disclose a gateway configured to provide object-level access *control* between the managers and the managed objects at the individual object level so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects. Spencer is completely silent regarding object-level access control. Spencer's SNMP trap system, cited by the Examiner, identifies an object configured to represent a particular agent system and configures a trap alarm (col. 7, lines 35-57). Vuong provides a name service that collects, maintains, and disseminates unique identifiers and addresses for processes on a computer network. The Examiner seems to be implying that any form of object-level access necessarily includes object-level access *control* at the individual object level. However, object-level *access* can be provided *with or without* imposing object-level access *control*. Please see Applicants' Response to Final Action, filed January 28, 2008, pp. 35-41 for a more detailed discussion.

Regarding claims 20, 39, 59 and 60, Vuong and Spencer fail to disclose determining on a managed object level whether or not the manager application is allowed to receive an event generated by one of a plurality of managed objects or to send a request to the one of the plurality of managed objects as a function of the identity of the user of the manager application. Even if one interprets the cited entries of Vuong's database as managed objects, Vuong still fails to disclose anything regarding determining whether or not the de-registering agent can access the database entry. Instead, Vuong teaches only that the name service checks the agent's name against the database and if it is found, the entry is removed. Spencer describes, at the Examiner's cited passage, managed application 300 communicating with a MIS server via the PMI interface allowing access to object instance state information, class schema and event services, which does not include or disclose determining whether a manager application is allowed to receive an event or send a request, as a function of the identity of the user of the manager application. Please see Applicants' Response to Final Action, filed January 28, 2008, pp. 35-41 for a more detailed discussion.

The Examiner rejected claims 1, 20, 39, and 58-60 under 35 U.S.C. § 103(a) as being unpatentable over Barker, et al. (U.S. Patent 6,363,421) in view of Barry et al. (U.S. Patent 6,615,258) (hereinafter "Barry") and JIDM Interaction Translation, Initial Submission to OMG's CORBA/TMN Internetworking RFP (hereinafter CORBA/TMN). Applicants traverse this rejection for the reasons below.

Regarding claims 1 and 58, the combination of Barker, Barry and CORBA/TMN fails to teach or suggest a gateway configured to **provide object-level access control** between the one or more managers and the managed objects to receive the one or more events from or to send the one or more requests to the managed objects, where the **object-level access control is provided at an individual object level** so that one or of the one or more managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects. Barker, as relied on by the Examiner, discloses "a method of *client based* access control of network elements" including "access control based on client name and password" (emphasis added, col. 8, lines 45-46 and col. 30, lines 45-46). Further, Barker summarizes, "the *client based access control* … provides a means to restrict access on a *command/client basis*" (emphasis added, Barker, column 31, lines 10-12). Moreover, Barker's use of EMAPI, CORBA, Java, C++ and SNMP, even in view of Barry and CORBA/TMN, does not imply any sort of object-level control for delivering events to or receiving requests from managed objects, even if combined with the other cited art. Additionally, "object-level control" (as stated by the Examiner) is not the same as "object-level *access* control" (as recited in claim 1). Controlling an object and controlling access to that object are two very different things. In the Advisory Action, the Examiner appears to argue that use of use of an object identifier necessarily includes providing object level access control (p 3, lines 10-17). However, Barker (as well as the other cited references) uses object identifiers as means of object addressing (e.g., to identify a particular element from among others). It is unclear how the Examiner's reliance on Barry for "usage at individual object level" relates to object-level access control since Applicants' claim does not recite "usage at individual object level." The Examiner's reliance on CORBA/TMN for "access control" is also misplaced because CORBA/TMN uses *domain-based access control* in which objects (both managed and manager) are grouped into domains and that domains "are considered the unit of accessibility" and "may have any number of objects within" them (CORBA/TMN, page 2-8, paragraph 7).

Furthermore, the Examiner's proposed combination of Barker, Barry and CORBA/TMN results in the CORBA-based remote management system of Barker, that utilized the graphical user interface as taught by Barry and that also includes domain-level access control as taught by CORBA/TMN. As shown above, Barker, Barry and CORBA/TMN all teach access control that is specifically not provided at an individual object level. The access control of Barker is at the client level, Barry's is at the user level, and the access control of CORBA/TMN is at the domain level. Moreover, the Examiner is simply identifying features of Applicants' claimed invention in disparate references while attempting an piecemeal reconstruction of Applicants' invention in hindsight without considering the claimed invention as a whole. The Examiner's stated reasons for the combination are not found in, or supported by, any evidence of record and thus can only have come in hindsight from Applicants' own teachings. Please see Applicants' Response to Final Action, filed January 28, 2008, pp. 35-41 for a more detailed discussion.

Regarding claims 20, 39, 59 and 60, the combination of Barker, Barry and CORBA/TMN does not teach or suggest determining on a managed object level whether or not the manager application is allowed to receive an event generated by one of a plurality of managed objects or to send a request to the one of the plurality of managed objects as a function of the identity of the user of the manager application. The Examiner refers to Barry's use of EMAPI, CORBA, Java, C++, and SNMP. However, the Examiner assumes incorrectly that Barker's use of CORBA and the IIOP protocol includes object level access control at the individual object level, when in fact, Barker's system involves *client based* access control and provides a means to restrict access on a *command/client basis* rather than at the individual object level, as recited in Applicants' claim. Please see Applicants' Response to Final Action, filed January 28, 2008, pp. 35-41 for a more detailed discussion.

The Examiner rejected claims 1, 20, 39 and 58-60 under 35 U.S.C. § 103(a) as being unpatentable over Barker in view of Barry and Buckle, et al. (hereinafter "Buckle").

Regarding claims 1 and 58, as discussed in Applicants' Response to Final Action, pp. 23-31, Barker, Barry and Buckle fails to teach or suggest a gateway configured to provide object-level access control where the object-level access control is provided at an individual object level, as recited in Applicants' claims. The

Examiner refers to Barker's use of EMAPI, CORBA, Java, C++ and SNMP, which, as shown above, fail to teach or suggest any sort of "object level control". The Examiner also relies on Buckle to teach, "access control so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects." However, none of the Examiner's cited figures illustrates any sort of access *control*. The Examiner is confusing providing "access" with providing "access *control* so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects". Barker and Barry teach access control that is specifically <u>not</u> provided at an individual object level (Barker at the client level and Barry at the user level), while Buckle fails to teach any access control whatsoever.

Moreover, as noted above, the Examiner identifies features of Applicants' claimed invention in disparate references for a piecemeal, and therefore improper, reconstruction of Applicants' invention in hindsight without considering the claimed invention as a whole. Furthermore, Barker's teachings are incompatible with the Examiner's combination. Barker teaches that once a client has been properly authenticated at the start of a session, that client may then register for attribute update notification for a number of managed objects through a single call (Barker, column 25, lines 27-28). Such functionality is clearly <u>not compatible</u> with *object-level* access control, as recited in Applicants' claim. Please see Applicants' Response to Final Action, filed January 28, 2008, pp. 23-31 for a more detailed discussion.

Regarding claims 20, 39, 59 and 60, the combination of Barker, Barry and Buckle does not teach or suggest <u>determining on a managed object level whether or not the manager application is allowed</u> <u>to receive an event</u> generated by one of a plurality of managed objects <u>or to send a request</u> to the one of the plurality of managed objects as a function of the identity of the user of the manager application. The Examiner relies on Barker's use of EMAPI, CORBA, Java, C++, and SNMP. However, as noted above, the <u>Examiner is incorrectly assuming</u> that Barker's use of CORBA and the IIOP protocol includes object level access control, as recited in Applicants' claim. Moreover, Barker in view of Barry and Buckle fails to teach or suggest that <u>**access for the manager application to receive the event or send the request is approved or denied** for said one of the plurality of managed objects **at the individual object level** so that the manager application is granted access to one of the plurality of managed objects while being prevented from interfacing with a different one of the plurality of managed objects</u>. Instead, Barker, even in view of Barry and Buckle, discloses *client based* access control that "provides a means to restrict access on a *command/client basis*" (emphasis added, Barker, column 31, lines 10-12). Barker does not describe his access control features as restricting access at the object level, even when combined with the other cited art. Please also see Applicants' Response to Final Action, filed January 28, 2008, pp. 31-33 for a more detailed discussion.

The Examiner rejected claims 1, 20, 39 and 58-60 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-39 of co-pending Application No. 09/552,984, over claims 1-44 of U.S. Patent 6,839,748, over claims 1-30 of U.S. patent 6,813,770, over claims 1-34 of

U.S. Patent 6,915,324 and over claims 1-34 of U.S. Patent 6,950,935. Applicants traverse these rejections on the grounds that the Examiner has not stated a proper *prima facie* rejection. As described in detail in Applicants' previous response (Response to Final Action, filed January 28, 2008, pp. 2-7), the Examiner has not listed ALL the differences between each rejected claim and the claims of the cited patent applications, nor given reasons, for each difference, why a person of ordinary skill in the art would conclude that the invention defined in the claim is an obvious variation of the invention defined in a claim of the other patent/application, as required for a *prima facie* rejection (MPEP 804.II.B.1). Instead, the Examiner improperly lumps all the claims together, without addressing each specific difference, while relying on broad generalizations of the claimed subject matter.

The Examiner provisionally rejected claims 1-60 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1- 39 of copending application 09/552,984, and over claims 1-45 of co-pending application 09/557,068. If and/or when these rejections become non-provisional, Applicants will consider filing a terminal disclaimer or present reasons traversing the rejection. The Examiner also rejected claims 1-60 under 35 U.S.C. § 112, second paragraph, as being incomplete "for omitting essential steps/elements/structural cooperative relationships of elements, such omission amounting to a gap between the steps/elements/necessary structural connections". Applicants respectfully traverse this rejection for at least the following reasons. The Examiner is improperly attempting to require recitation of a specific and particular embodiment described in Applicants' specification. The elements and/or structural connections referred to by the Examiner are not necessary or essential to implementing or accomplishing Applicants' invention. They are, in contrast, described simply as one embodiment in Applicants' specification, not as the only possible implementation. The Examiner is improperly attempting to require recitation of a specific and particular embodiment described in Applicants' specification. Please refer to Applicants' previous response dated January 28, 2008, pp. 8-10 for a more detailed discussion.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicants hereby petition for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert & Goetzel PC Deposit Account No. 501505/5181-48400/RCK.

Respectfully submitted,
/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850
Date: February 28, 2008